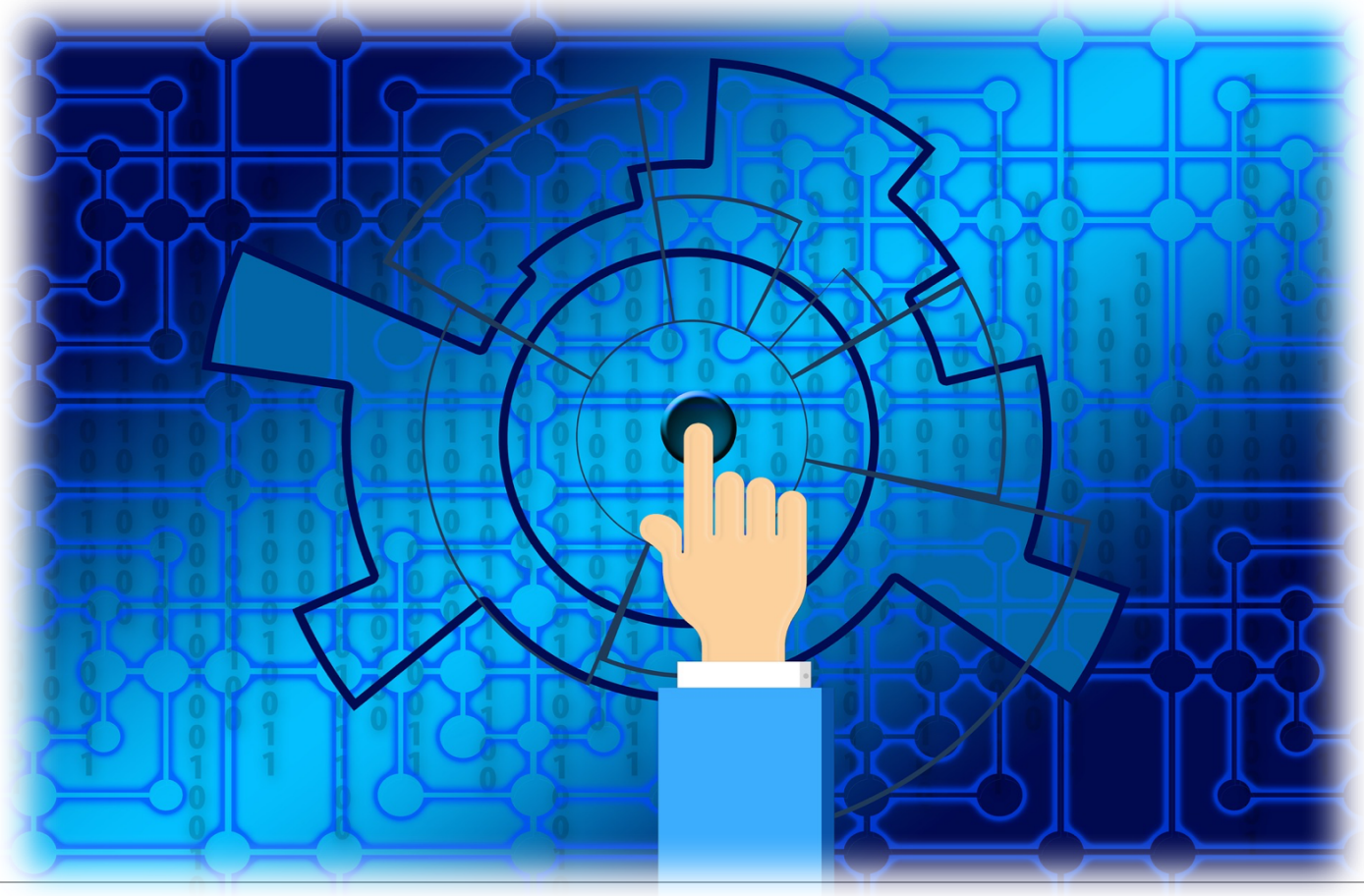
Challenges for the Legal Profession: Data Management, Confidentiality and Cyber Security

Dominique Hogan-Doran SC
Senior Counsel of the New South Wales Bar

FIJI LAW SOCIETY ANNUAL CONVENTION 2017

1 SEPTEMBER 2017



CHANGING LANDSCAPE OF THE LEGAL PROFESSION

Profession Reviews

- **USA**: 20/20 Commission; ABA Commission on the Future of Legal Services
- **Europe**: Council of the Bars and Law Societies of Europe (CCBE), Future of the CCBE and of Legal Services Working Group
- **Canada**: Legal Futures Initiative
- **UK**: Bar Standards Board and ILEX Professional Standards, Legal Education & Training Group

A portrait common to the professions

- Specialist knowledge
- Admission depends on credentials
- (Exclusive) activities regulated
- Bound by common set of values

A portrait: the good

- Knowledgeable
- Expert
- Skillful
- Know-how

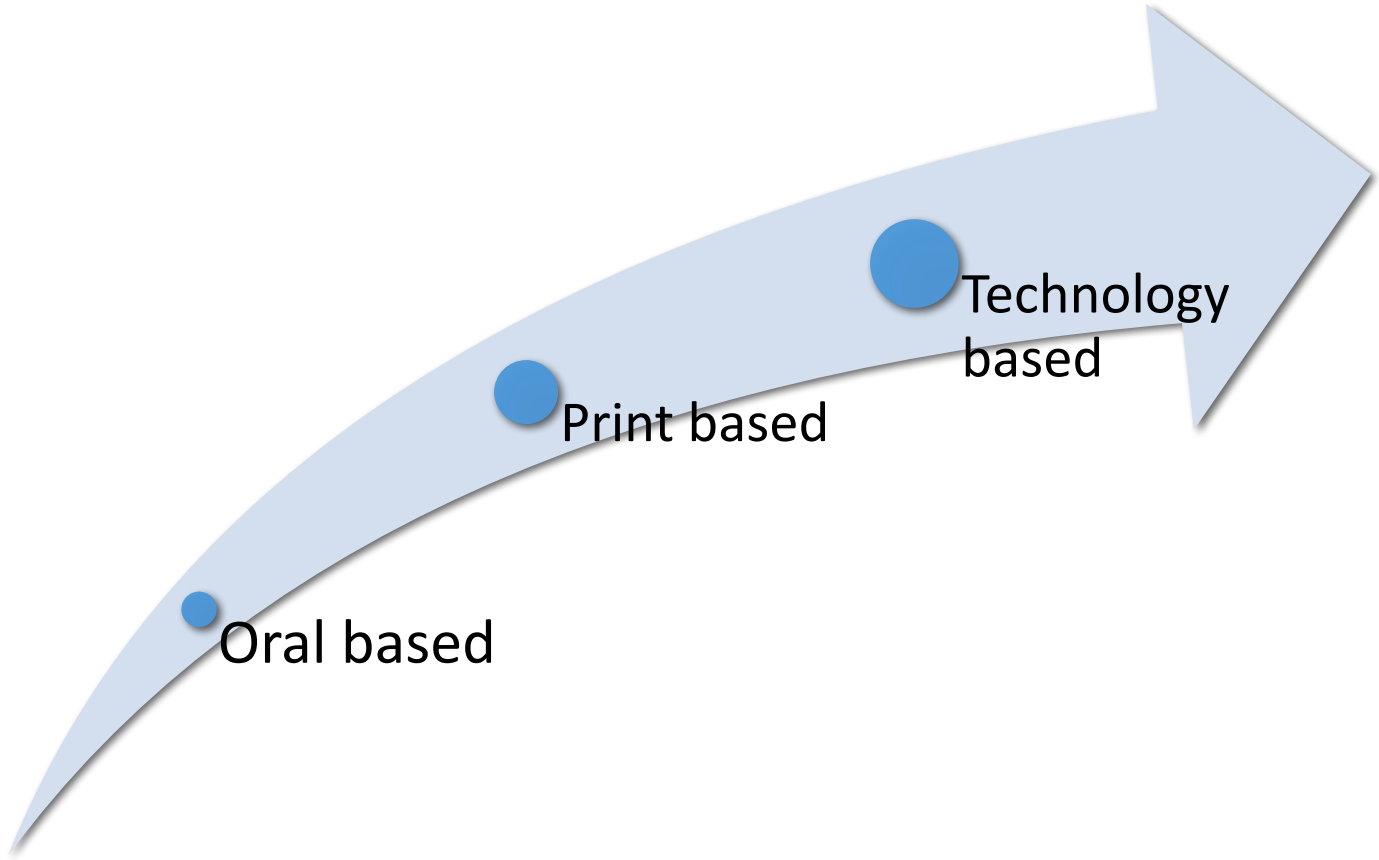
A portrait: the bad

- Unaffordable
- Antiquated techniques
- Under-exploiting technology
- Expertise of best enjoyed by few
- Underperform

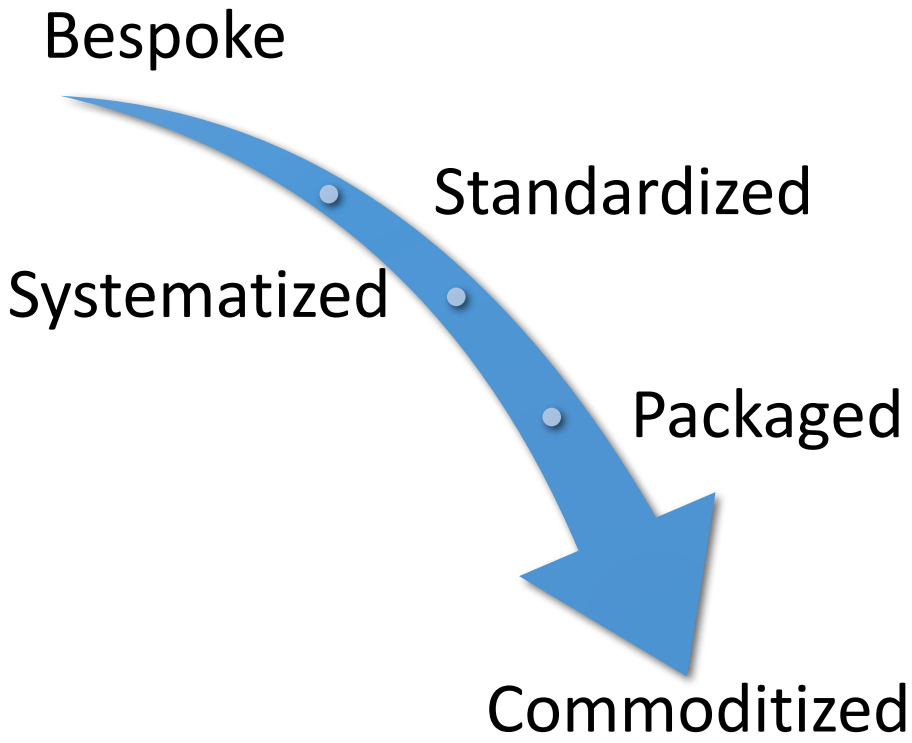
A portrait: the ugly

- Ethically challenged
- Nontransparent
- Inscrutable
- Disempowering

Evolution of legal services



Evolution: Legal Services



TECHNOLOGY *HELPS* LAWYERS PRACTICE LAW

Technology *helps* lawyers practice law

- Better manage information
- Streamline legal practice
- Access information
- Lower overhead costs
- Minimize time spent on administrative tasks
- Handle more cases
- More easily connect with potential clients
- Work collaboratively with existing clients

Litigation, decomposed

document review

legal research

project management

litigation support

(electronic) disclosure

strategy*

tactics*

negotiation

advocacy*

Transactions, decomposed

due diligence
legal research
transaction management
template selection
negotiation
bespoke drafting
document management
legal advice
risk assessment

We have the technology

automated document assembly

relentless connectivity

electronic legal marketplace

e-learning

online legal guidance

legal open-sourcing

workflow and project management

Cloud Computing is a *key* technological advance

- Do you use Hotmail? Gmail? iCloud? DropBox?
- You are already using cloud computing!
- Remote servers belonging to a third party and accessed over the Internet.
- Stores and manages data, rather than a local server or a personal computer.
- Importance of cloud computing is the *international* dimension.

Confidentiality obligations means securing client information is *vital*

- Data stored in different locations increases the area for possible attacks.
- A hacker or malware could potentially access data as it moves over multiple networks.
- Service providers may deal with deleted files in different ways – client files may be hidden on a site's servers rather than being permanently deleted.

Personal professional duty?

- Comment 8 to Model Rule 1.1 provides:

  "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

- On January 1, 2017, Florida first state to require **technology training** as part of its CLE requirement.

- Attorneys licensed in Florida must obtain 3 additional hours of technology CLE during each 3-year reporting cycle.

Cyber Security

The Threat Landscape

- Malware - viruses, Trojans, worms, spyware, keyloggers, backdoors
- Phishing
- Ransomware – *Wannacry*
- Weak and default passwords
- Outdated or unpatched software vulnerabilities
- Removable media – thumbdrive, USB, external hard drive, DVD, CDs

Lawyers are affected too!

- Hacking of files of Panamanian law firm Mossack Fonseca demonstrates extraordinary consequences of data breaches for law firms and their clients.

- Ransomware attacks are expensive for legal practitioners:
  - Financial costs
  - Risks to client confidentiality
  - Reputation risks
  - Regulatory risk

Security Mindset

- Digital and cyber security is an issue of *culture*.
- Lawyers must have a mindset where individual is ultimately responsible for the security of client information.
- Lawyers cannot assume someone else is going to take care of information.
- If a lawyer does not think that their client's information is sufficiently protected, they should take active steps to obtain guidance.

Key Cyber Security Risk Areas

- **IT systems** – what are they? how secure are they?
- **Staff** – what training? password sharing? insider threat?
- **Sub-contracting** (including cloud based services) – due diligence? contracting?
- **Unconscious cloud computing** – Hotmail? Gmail? Dropbox? Mobile apps?
- **Personal computing and devices** – BYOD policy in place?
- **Remote and mobile workforce** – personal email? unsecure connections?

Don’t be the Pebkac: The 7 Pillars of Digital Security

1. **Physical** and **digital locks** ensure access to information when you have temporarily parted possession *deliberately*
2. **Location tracking** ensures access to information when you have temporarily parted possession *inadvertently*
3. **User authentication** regulates the *authorised* disclosure of information
4. **Encryption** prevents the *unauthorised* disclosure of information
5. **Data deletion** prevents *unauthorised* and *inadvertent* disclosure of information
6. **Backup** prevents *inadvertent* destruction of information
7. **Pebkac** prevents the *ineffectual* disclosure of information

Tips for Remote or Mobile Working Lawyers

(1) **Bring your own** – ensure mobile devices are switched to a trusted network (such as your employer's connection) not to Wi-Fi

(2) **Use HTTPS** – HyperText Transfer Protocol Secure offers more security than HTTP

(3) **Disable file sharing** – this is a key way a hacker can infiltrate your system when using public Wi-Fi

(4) **Use a Virtual Private Network** – VPN helps prevent anyone from intercepting your internet traffic and it also cloaks your device's IP address

(5) **Use your own personal VPN** – use OpenVPN to install reliable firmware that encrypts and secures data

Tips for Remote or Mobile Working Lawyers

(6) **Privacy Extensions –** protects from material you download, and blocks third party tracking cookies and prevents trackers from collecting your data

(7) **Antivirus and malware protection** – ensure your device has reliable and up to date antivirus and anti-malware software

(8) **Turn off Wi-Fi** – if you don't need to remain connected to a public network, turn it off

(9) **Use a semi-open network** – if you have a choice of networks, consider a "semi-open" Wi-Fi option.

(10) **Don't use it**

Resources

- Philippe Doyle Gray, *The Pillars of Digital Security: How to ethically use technology in legal practice* (2017)
- Richard Susskind and Daniel Susskind, *The Future of the Professions: How technology will transform the work of human experts* (2015, Oxford University Press)
- John Sammons and Michael Cross, *The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy* (2017, Elsevier)

Resources

- Mark Button and Cassandra Cross, *Cyber Frauds, Scams and their Victims* (2017, Routledge)
- Corey Schou and Steven Hernandez, *Information Assurance Handbook: Effective Computer Security and Risk Management Strategies* (2015, McGraw-Hill Education)
- Geoffry Holland, Kathryn Crossley and Wenee Yap, *Social Media Law and Marketing: Fans, Followers and Online Infamy* (2014, Thomson Reuters)

Comments/Questions?

DOMINIQUE HOGAN-DORAN SC

www.dhdsc.com.au

Twitter @DHoganDoranSC